UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

7590 02/19/2009

David B Cochran
Jones Day Reavis & Pogue
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/19/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/594,368	LITTLE, HERB A.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on November 25, 2008 has been entered.

Claims 1, 16 and 31 are amended.

Claims 1-45 are pending and herein considered.

Response to Amendments and Arguments

Applicant's claim amendments serve to overcome the Examiner's previously set forth 35 USC 112 rejections. As a result, those rejections are Withdrawn.

Applicant's arguments with respect to claims 1-45 and Schneier's failure to teach wherein the key pair used for encryption is the same key pair used to create a digital signature have been considered but are moot in view of the new ground(s) of rejection. Upon further search and consideration, the Examiner has discovered a number of references disclosing the dual use of a key pair for encryption and the creation of digital signatures. The Examiner has included with this office action two of these references, including a memo from Aram Perez of Apple Computer dated back to 1998 disclosing

this dual use. The Examiner has amended her rejection of claims 1-45 below to include the subject matter from the Perez memo.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al., US Pat 5,956,404 and further in view of Aram Perez' "Digital signature and non-repudiation key usage bits.

Regarding **Claims 1, 16, and 31**, Schneier teaches a public-key encryption process and system for communicating messages between a sender and a receive comprising the steps of for each message: a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message (see Schneier col.1 lines 28-44); and b) generating a digital signature for the ciphertext message using an ephemeral key pair (see Schneier col.1 lines 45-65); wherein the ephemeral key pair used in the encrypting and generating steps is used for a single message between the sender and the receiver.

Schneier fails to specifically disclose generating a digital signature using the key pair produced in the encrypting step.

Perez discloses using the same keys for encryption and digital signatures.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Schneier the dual pronged use of keys as described in Perez to allow for the repeated use of a key pair saving the time and resources that would normally be required in order to create a new key pair.

Regarding **Claims 2, 17, and 32**, Schneier and Perez teach a public-key encryption process and system wherein the encrypting step uses an El Gamal encryption scheme (see Schneier col.1 lines 45-65).

Regarding **Claim 3**, Schneier and Perez teach a public-key encryption process wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme; wherein the step of generating the digital signature includes hashing the plaintext message (see Schneier col.1 lines 45-65).

Regarding **Claims 18, and 33**, Perez and Schneier teach a public-key encryption process and system wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme (see Schneier col.1 lines 45-65).

Regarding **Claims 4, 19, and 34**, Perez and Schneier teach a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and

calculating an encryption ephemeral public key X = xG, where G is a generator (see Schneier col.1 lines 28-44).

Regarding **Claims 5, 20, and 35**, Perez and Schneier teach a public-key encryption process and system for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key a; and

b) calculating a sender public key A = aG, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key B = bG,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains an authentic copy of the sender public key A (see Schneier col.1 lines 28-44).

Regarding **Claims 6, 21, and 36**, Schneier and Perez teach a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key X = xG (see Schneier col.1 lines 28-44).

Regarding **Claims 7, 22, and 37**, Perez and Schneier teach a public-key encryption process and system, further comprising the steps of, at the sender, generating a secret key K = xB and encrypting a plaintext message using the secret key K to generate a ciphertext message (see Schneier col.1 lines 28-44).

Regarding **Claims 8, 23, and 38**, Perez and Schneier teach a public-key encryption process and system, further comprising the steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature (see Schneier col.1 lines 45-65).

Regarding **Claims 9, 24 and 39**, Perez and Schneier teach a public-key encryption process and system, wherein the digital signature comprises a first value r and a second value s, the process further comprising the step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver (see Schneier col.1 lines 45-65).

Regarding **Claims 10, 25, and 40**, Perez and Schneier teach a public-key encryption process and system, further comprising the steps of, at the receiver, generating the secret key K = bX = bxG = xbG = xB, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based on the calculated first value r and the transmitted second value s (see Schneier col.1 lines 45-65).

Regarding **Claim 11**, Perez and Schneier teach a the public-key encryption process of Claim 1, wherein at least a two-stage public-key encryption process is used; wherein the first stage includes key establishment and the second stage includes encryption/decryption; wherein said steps (a) and (b) are performed during the second stage of encryption (see Schneier col.1 lines 45-65).

Regarding **Claims 12-15, 26-30 and 41-45**, Perez and Schneier teach a public-key encryption process and system and its implementation in wireless hand-held communication devices within a communication system (see Schneier col.5 lines 8-40).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437